CYLON

• CYLON INSIGHTS •

SIGNAL FROM NOISE:

HOW TO WIN CUSTOMERS & INFLUENCE CISOS

{ISSUE 2}

TABLE OF **CONTENTS**

FOREWORD

Since 2015 the collective experience of CyLon and its global network of cybersecurity leaders has helped over 100 early-stage cyber companies build sustainable, scalable businesses. The knowledge, experience and guidance of our 350+ mentors continues to provide tremendous value to founders that join our global programmes.

Through this second issue of our ‘CyLon Insights’ series we want to share the wisdom of our mentors more widely. In this report we use data and opinions gathered from our network of senior cybersecurity decision makers to delve further into what makes a CISO tick.

Based on a comprehensive survey and subsequent interviews around product evaluation, buying habits, and organisational security needs, we aim to provide insights on the current priorities for CISOs, the product gaps in the cybersecurity market, and practical guidance to help cyber companies collaborate with their target customers.

We hope this report appeals not only to new vendors and cybersecurity decision makers, but that those right across the cybersecurity ecosystem - from budding entrepreneurs to industry veterans - find value and use in the findings.

KEY STATS

3 NEW SECURITY PRODUCTS PURCHASED EACH YEAR

1 1 REVIEW OF SECURITY ENVIRONMENTS PER YEAR

50+ NEW VENDOR PITCHES RECEIVED ANNUALLY

1-2 NUMBER OF HOURS PER WEEK CISOS SPEND REVIEWING PITCHES

75% OF RESPONDENTS SAID THAT LESS THAN A QUARTER OF PITCHES THEY SEE ARE "VERY GOOD"

RISK REDUCTION

The biggest priority for CISOs making technology decisions

NOT SOLVING THE PROBLEM

The main reason CISOs reject new vendor pitches

MULTI-POINT SOLUTIONS

What CISOs want most

UNCLEAR MESSAGING & LACK OF USP

The most common mistakes found in new vendor pitches

TOP PRIORITIES:

- Cloud security
- Threat detection
- Governance, risk & compliance

PART 1

WHAT CISOS BUY & WHY

WHAT ARE CISOS LOOKING FOR?

One of the most overused phrases in cybersecurity discourse is “the ever-changing landscape”. While it is true that security threats evolve alarmingly quickly, this doesn’t mean that the needs of CISOs, or the technology solutions they use, change at the same pace.

“Cybersecurity needs of businesses haven’t changed much in 25 years and we’re still looking for solutions to the same problems,” says Ollie Whitehouse, Chief Technical Officer at NCC Group, and CyLon mentor.

Not only are the needs of CISOs fairly consistent, but it also seems that CISOs don’t buy a huge amount; the survey confirmed that CISOs only purchase around three new products each year (median), independent of company size and sector.

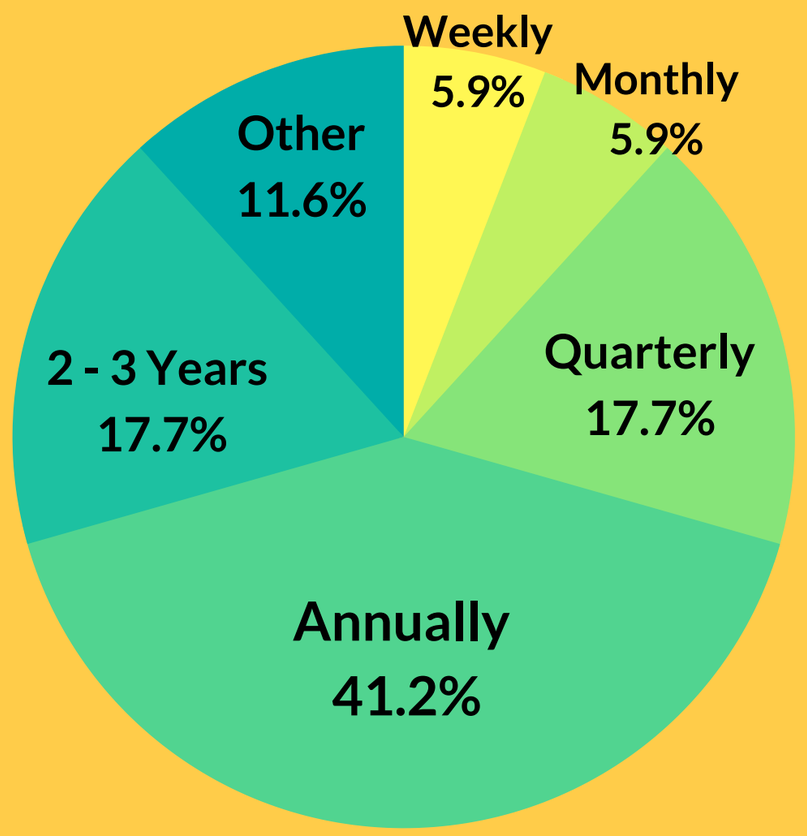
At one end of the scale for new product appetite, a global professional services company with between one thousand and ten thousand employees (and a security team of 70 to 50 people) buys only one new product a year.

But at the other extreme, a global consulting company with more than ten thousand employees and a huge security team of 420 people has an anomalously high number of product purchases: 50 a year.

Importantly, companies tend to only review their security technologies once a year, and worryingly some only reevaluate after a security breach.

3

NEW SECURITY PRODUCTS PURCHASED EACH YEAR



HOW OFTEN COMPANIES REVIEW THEIR SECURITY TECHNOLOGIES

Just under 60% conduct an audit annually (41%) or every two to three years (18%). And most CISOs say that their decisions to buy new products are almost always the result of a continuous process of monitoring and analysing how technology and security threats are evolving, rather than concerted efforts to find a specific solution.

Many business processes could reasonably be counted within the cybersecurity remit - from physical device management to high-level business continuity strategies.

Not all of these areas require third-party technology products. In fact, CISOs' primary technology needs are currently concentrated in three main areas: **cloud security, threat intelligence** and **governance, risk and compliance.**

Cloud security

The uptake of public cloud in the last few years has also increased the need for security expertise in business decision-making. But too often security has been an afterthought to cloud migration, leaving CISOs scrambling to understand the security situation on their hands.

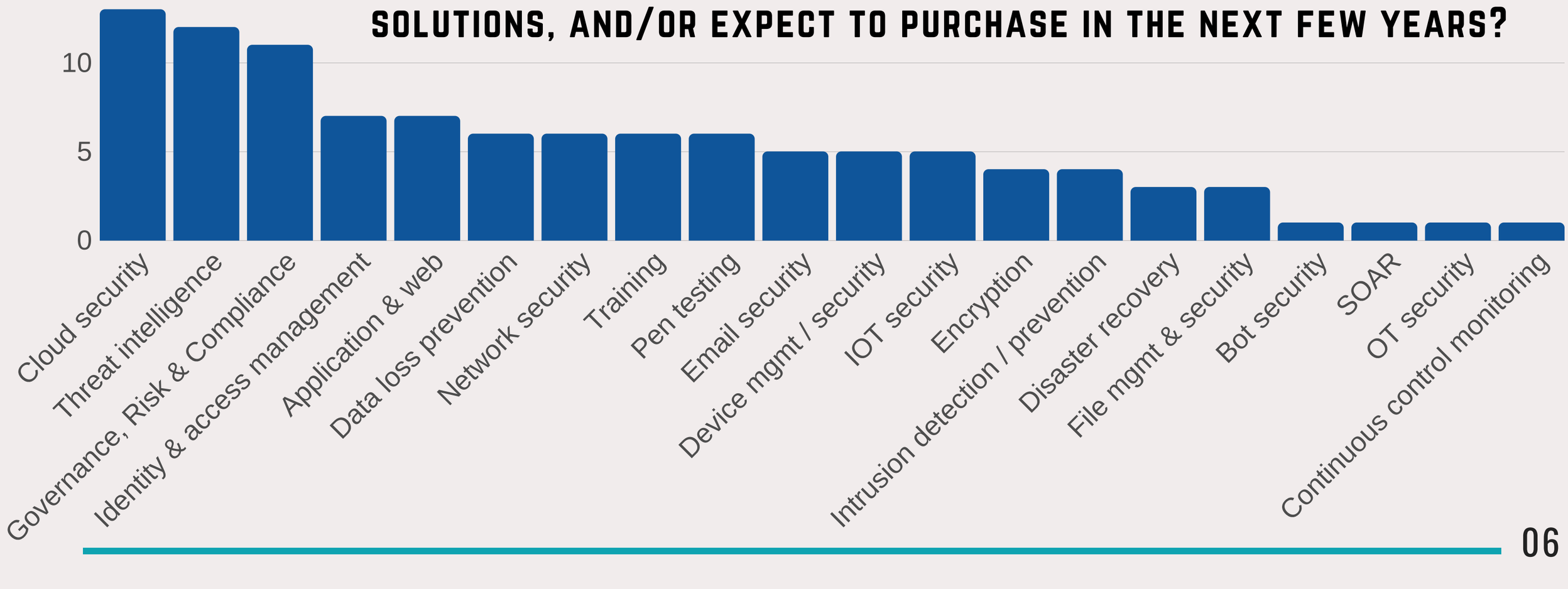
> ***Businesses are expanding into the cloud in a rapid way, and security leaders have not always been at the table when the decision was made to go into the cloud.***
>
> *- Paul McKay, Senior Analyst at Forrester Research.*

"CISOs are not even sure what cloud applications are in use by the business, what is considered sanctioned or unsanctioned. Getting that visibility is one of the big challenges", says Paul McKay. Cloud services are distributing the technology resource and control across businesses, but inevitably the trade-off is that security vulnerabilities and risks also increase as CISOs lose central oversight.

The demand for cloud security also exposes an inconvenient truth: vendors are not keeping up with cloud security needs, particularly when it comes to agile deployment on the cloud, like microservices and containerless architecture, and key security.

WE ASKED:

WHICH AREAS OF CYBERSECURITY ARE YOU CURRENTLY LOOKING AT FOR SOLUTIONS, AND/OR EXPECT TO PURCHASE IN THE NEXT FEW YEARS?



"The current state of encryption technology makes it quite hard for a security-conscious outfit like a bank to have confidence that the encryption keys are solely under their control," says Alan Jenkins, Head of Advisory Services at 2|SEC Consulting.

"There is an element of risk acceptance to trust the cloud provider. Since you have no control over physical access to the servers in the cloud provider's data centre, the security of encryption keys becomes essential."

The 'time lag' between CISO needs and cloud security products coming to market could be an important opportunity for security startups who can specialise from the outset, while legacy providers are somewhat encumbered by the scale or variety of their own product portfolio.

"Even if you do find the right vendor to work with for cloud security, is that vendor agile enough to keep up with the pace of innovation?" asks Paul McKay. "That's where startups have the opportunity to come along and demonstrate a different way of looking at a problem."

> ***"For startups, it is prudent to keep up with what's on the agenda for regulators and policy-makers; those are the areas that will soon become a priority for CISOs."***

Threat intelligence

Despite being the second-most sought after area for technology solutions, threat intelligence technology divides opinions among CISOs. In theory, the more a business can understand its cyber threats, the better it can prepare and protect itself. But in practice, intelligence from analytics platforms cannot be consumed or acted upon.

Insights from threat intelligence products currently on the market range from macro themes (i.e. geopolitical trends or newly discovered exploits) to information about specific attacks, attackers, targets and vulnerabilities. For the most part, only the latter directly impacts a CISO's day-to-day work. Best-of-breed threat intelligence solutions already provide these insights, but it comes at a high cost.

Nonetheless, others do see the value of threat intelligence, and say that understanding the basics of 'know your enemy' can be applied to business actions.

"There are limits to what you can do with threat intelligence," one respondent admits. "You can't do anything about attackers' motivations but hopefully you can do something about the methods they use. At the end of the day it comes down to managing your vulnerabilities and making sure you have a response."

It might not be as "sophisticated" as geopolitical information sounding the alarm about imminent attacks, but the future of cybersecurity relies on improving machine-detection of security breaches and indications. This is where one respondent sees the value of threat intelligence, by feeding "indicators of compromise" into other security tools to enhance the accuracy.

For this to happen, threat intelligence must evolve from macro reports to machine-readable signals, says Joshua Kennedy-White, a cybersecurity consultant at Accenture in Singapore.

"The threat intel models must be able to be read by our systems and acted upon at machine speed," he says.

Governance, risk and compliance

Governance, risk and compliance (GRC) was named as one of the key areas for which CISOs want to see more startups developing security solutions. But unlike other product areas, GRC is felt to be somewhat disconnected from actual security challenges.

Instead, CISOs say, compliance solutions are important because regulators, customers and other stakeholders want to see businesses proactively monitoring their risks and taking governance seriously.

Unfortunately, demonstrating compliance is not always an indicator of effective security and risk management.

> ***"Compliance is a necessary evil, but it doesn't make you secure," says Alan Jenkins. "It depends which standards you are compliant with."***

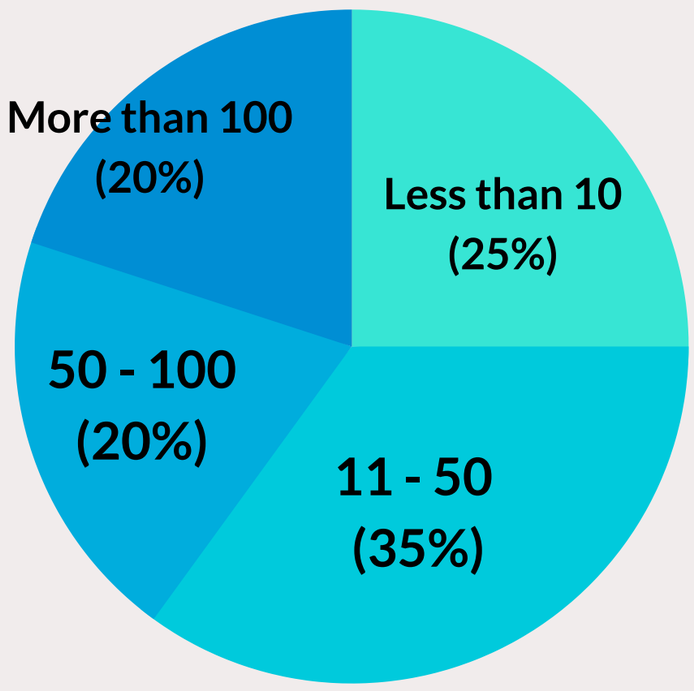
On the other hand, compliance tools do not come cheap, outweighing the value of a "box-ticking exercise", which is how some CISOs refer to GRC. The cost of technology tools would not be worth spending if the company was only using the solutions to prove compliance to others. Another approach is to see the business case for compliance tools: they help CISOs quantify operational risks and then assign and justify the amount of money they should spend to mitigate them.

For startups, it is prudent to keep up with what's on the agenda for regulators and policy-makers; those are the areas that will soon become a priority for CISOs. The pace of regulatory change means that a simple and effective solution to meet new requirements could be extremely successful.

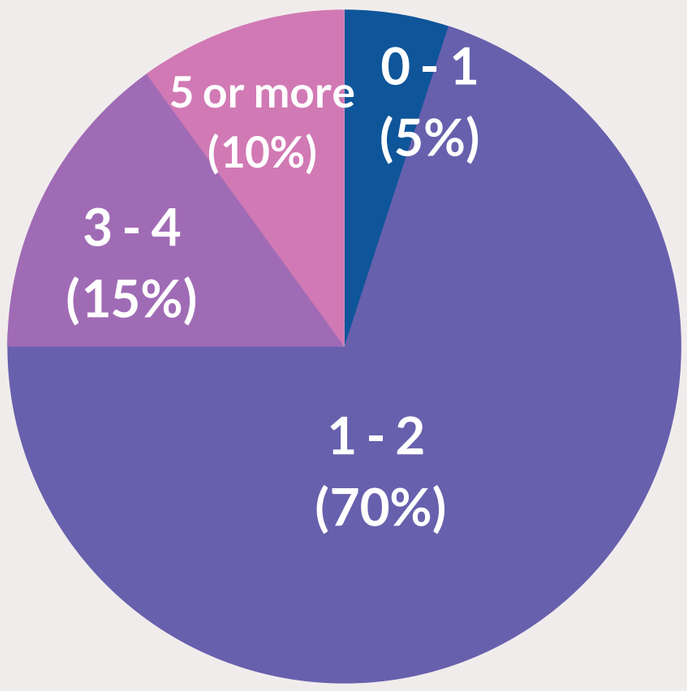
HOW DO CISOS MAKE BUYING DECISIONS

CISOs are inundated with product pitches; 40% read more than 50 pitches annually, averaging to a new vendor pitch each week. Some security officers are consuming more than one a day: 20% read or hear more than 100 annually and the highest response was "300-400 pitches per year".

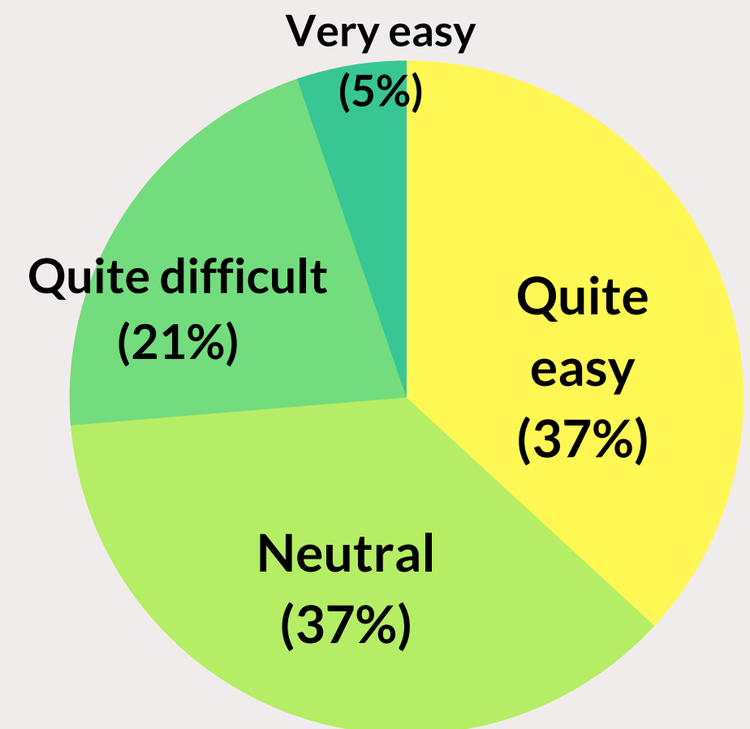
This can be explained by the fact that there is one clear priority for CISOs making technology decisions: risk reduction. Two-thirds say it is the most important factor when evaluating products, compared to 5% who said cost was the most important factor and just under 30% who chose user experience as a top priority.



We asked: "How many security vendor pitches do you read / hear on average every year?"



We asked: "How much time can you dedicate to reviewing new vendor products / pitches?" (hrs/week)



We asked: "How easy / difficult is it for you to evaluate and select the cybersecurity solutions your company needs?

The majority of CISOs (70%) are spending only an hour or two each week reviewing pitches, and a set maximum of five hours. One respondent said “I am only supposed to take a maximum of five hours of vendor briefings a week. This is time reserved for taking briefings on new products or updates to existing products.”

But CISOs don’t particularly struggle to select the new products they want to go ahead with. On a scale from “very easy” to “very difficult”, 37% of CISOS say it is “quite easy” to evaluate and select the cybersecurity solutions their companies need.

“The price is immaterial if the solution works,” says one respondent. “As long as the cost is proportionate to the problem it is solving, then what matters is how effective the product is.”

For Joshua Kennedy-White, the 'BANT' sales evaluation method is a useful framework for cyber products: budget, authority, need and timeframe.

Timeframe is more than just time to implement a new solution across the business; more importantly, under-resourced CISOs are seeking solutions that won’t be an ongoing burden to manage.

Two-thirds of CISOs said that the time and resource it would take to manage a product is one of the top two decision factors.

Even though the evaluation process isn't overly difficult for CISOs, they would like to see some key developments in the vendor landscape to make the process more manageable and efficient.

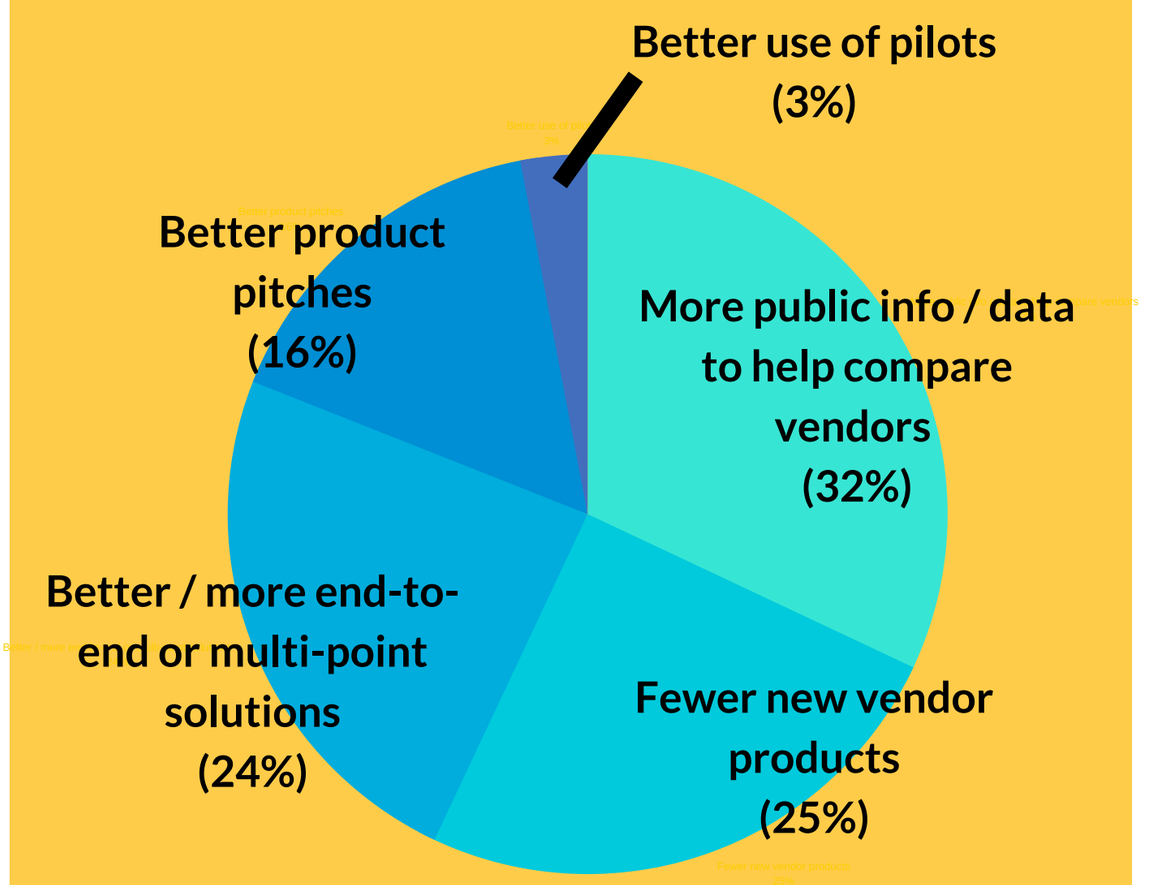
METRICS USED IN DETERMINING THE VALUE OF NEW SECURITY SOLUTIONS, IN ORDER OF IMPORTANCE

1. Risk reduction
2. Time / resource from my team to manage
3. User experience
4. Integration time
5. Cost

Vendor noise is complicating decision-making, and so 32% want more information to help them sift through and compare products.

WE ASKED:

WHAT WOULD IMPROVE THE PROCESS OF EVALUATING VENDORS?



When asked, CISOs say they would much rather see independent third-party product testing than benchmarking or crowd-sourced user reviews.

But Ollie Whitehouse points out that there are challenges for third-party companies trying to offer this service, following a legal battle between product tester NSS Labs and vendor Crowdstrike over negative product reviews.

"A marketplace to discover new products, coupled with performance scores for product efficacy, would be truly valuable," he says. "But I'm mindful that we've seen litigation on behalf of vendors when they are assessed in this manner."

THE COST FACTOR

Price point might not be the most important factor, but budget does determine which opportunities a CISO can consider.

And budget does vary greatly between different company sizes and sectors. Companies with more than a thousand employees spend up to £2m on cyber products, and companies with more than 10,000 employees generally spend multiple millions. Financial services firms are willing to spend the most on security, up to £5m a year.

In regions like Singapore and Australia, where the cybersecurity and finance communities are smaller but extremely active, CISOs tend to know how much their peers spend on security products, and so there is some convergence on budgets.

“If you are selling a cyber product to the banking community in a market like Australia or Singapore, you have to know that the CISOs all talk,” says Accenture’s Joshua Kennedy-White.

> ***More than half (53%) said they have too many security technologies in their environment at the moment.***

THE "SILVER BULLET"

A recurring theme that surfaces in every discussion with CISOs about their product gaps and needs is that they would like to see more multi-point or end-to-end solutions. A quarter said that would improve their decision-making process, and multi-point products were jointly chosen as the area in which CISOs want to see more offerings (16%, along with Governance, Risk and Compliance products).

More than half (53%) said they have too many security technologies in their environment at the moment.

But what exactly does the ideal, comprehensive, end-to-end cybersecurity product look like?

WE ASKED:

WHAT IS YOUR SUGGESTION FOR DREAM CYBER SOLUTIONS WHICH DON’T YET EXIST?

- An integrated threat management and machine speed remediation
- There is no silver bullet. We have a dynamic, fast-changing, unpredictable environment and it's dangerous to suggest there is one solution that can keep up
- Active vulnerability management solutions (self healing management systems)

The most comprehensive description of the “silver bullet” product was:

> ***A platform for real-time views of all IT assets grouped by business services, linked to business risks and controls with a real-time view of control effectiveness, and the ability to attach incidents to specific assets to assist with investigation/remediation prioritization.***
>
> ***Essentially a combination of GRC, threat intel, incident response, and continuous controls monitoring in one.***

Currently, these “holistic” solutions are being assembled from tools that were designed for more specific tasks or environments, which could cause problems.

But many respondents disagreed that a single "silver bullet" solution exists.

Paul McKay explains: “There isn’t a single solution that does it all very well, but there are particular solutions that do part of the puzzle very well.”

Rather than a single multi-point solution, more vendors are working on points of integration with other products, in response to demand from CISOs. Even large and established vendors are now committing to interoperability through APIs and shared protocols so that specific cyber tools can all sit within an integrated solution structure.

As Phil Owen, CISO of Tesco Bank, put it, “There is no silver bullet. We have a dynamic, fast-changing, unpredictable environment and it's dangerous to suggest (especially to your Board) that there is one solution that can keep up and "fix" cybersecurity".

PART 1: FINAL REMARKS

The survey highlighted that CISOs are inundated with new vendor pitches, yet rarely can they dedicate much of their time to reviewing the products. This means startup vendors have an extremely limited window of opportunity to sell to them.

The survey also uncovered some prominent themes around CISOs' changing needs to manage and have oversight over more flexible, modular cloud environments, and a demand for multi-point or interoperable solutions. Subsequent interviews with CISOs revealed that there are always at least two sides to all these themes, since CISOs have to straddle technology and strategy, always seeking to reduce day-to-day risk and vulnerabilities while also planning ahead for future innovations.

Understanding this delicate balance, and particularly the importance of business strategy in a CISO’s role, is the only way for vendors and startups to effectively meet their needs, as we’ll discuss in the next section.

WE ASKED:

WHAT ARE THE BIGGEST MISCONCEPTIONS AROUND A CISO'S JOB

People think CISOs need more technology, but we don't. What we need is better visibility and insights in order to make more informed decisions.

That CISOs are all the same. We aren't: we are diverse in our focus and skills. Some of us are very techy, some of us are very risk-focussed, some are more leadership-focussed. A startup needs to know which CISO "type" they are selling to and adapt accordingly.

People think some shiny new tech will be hugely interesting. CISOs have a million (generally boring, but urgent) challenges every day. Help us put out the fire before expecting us to evaluate some new tech.

WE ASKED:

HOW WILL THE CYBERSECURITY ENVIRONMENT & NEEDS OF BUSINESSES CHANGE IN THE NEXT FIVE YEARS?

Boards will need to stop fixating on the cost of cybersecurity and start thinking about the cost of not prioritising cyber.

Needs will be shaped by the threat environment. AI will be a key factor in defence (it's already being used in attack). I think the right solution will be one that covers the entire risk/value chain – this doesn't exist today.

The balkanisation of the internet: if you are a multinational and you are having to operate in Russia, China and America/Northern Europe, then you will essentially be working across three different internets. That will have an impact on how you do business.

The CISO role will continue to evolve into a clear leadership role, rather than purely tech or risk-focused.

PART 2

GET THEIR ATTENTION

PART 2

GET THEIR ATTENTION

It is notoriously hard for startups to break into an established marketplace, and there are additional challenges for cyber startups, who aim to sell into a world that is premised on secrecy and access control.

So how can startups succeed within a culture of risk management rather than the more common “move fast and break things” approach to innovation?

Practical advice can be gleaned from the insights from our CISO survey in three fundamental areas: **how to get a new product in front of CISOs; how to conduct pitches and conversations when you have managed to get a CISO’s attention; and how to make sure you are providing what CISOs really need.**

GETTING A NEW PRODUCT IN FRONT OF A CISO

CISOs are sometimes proactively seeking out a specific solution or technology, and many look to cyber accelerators, attend demo days, and spend time “round the edges” of security conferences, in small innovation zones rather than the main expo strip.

CyLon was among the the most-mentioned methods of finding product “gems”, which speaks to the value that programmes like CyLon's provide to time-stretched CISOs. By keeping up with cyber accelerators, events and funding news, CISOs are essentially outsourcing the first stage of finding new vendors to other experts, and then selecting from within an already-approved bunch.

Specifically, CISOs mentioned that they make a note of startups winning cyber awards, and use resources like Cyber Startup Observatory and M&A updates from consultancies such as Momentum Cyber.

Some of these sources of attention cannot be impacted by even the most proactive startups, but it is important for startups to focus marketing and sales energy, time and budget in the right place. This means attending the right events (Ignite, BlackHat and RSA Conference to name just three), applying to appropriate accelerator programmes and networking.

No CISO finds their next purchase from a cold-call or a cold-pitch, so startups would do well to steer clear of these more traditional product sales techniques.

> ***“The best way for a startup to get my attention is if they come recommended from a peer or friend. I also value authenticity over anything else; as soon as I question your credibility, you've lost me.”***
>
> *- Phil Owen, CISO, Tesco Bank*

"The best way for a startup to successfully get my attention is if they are succinct and don't require a meeting to give me basic information," says Ollie Whitehouse.

"Attach a meaningful set of slides to an email which allow me to get a good sense of what the solution is, how it has been put together, how it works and what its efficacy is."

KEY TAKEAWAYS FOR STARTUPS

DON'T

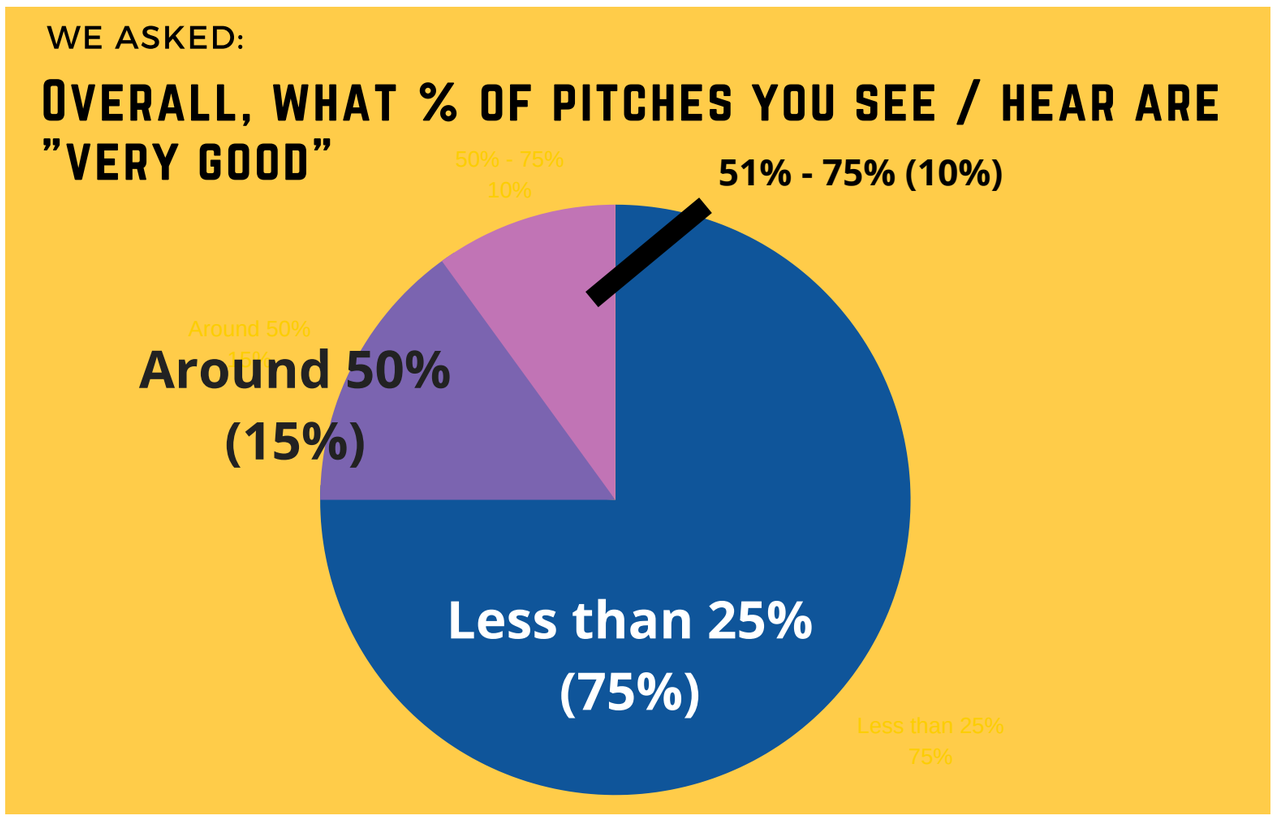
- **Cold call/email CISOs with a sales pitch**
- **Request a meeting to give information that could be summarised as an email attachment**
- **Forget the importance of first impressions**

DO

- **Apply for cybersecurity accelerators and awards**
- **Get involved at innovation events at the big conferences**
- **Network with security leaders even if they are not a direct sales opportunity**
- **Highlight referral clients and efficacy results of product testing**

HOW (NOT) TO PITCH

An overwhelming proportion of cybersecurity pitches miss the mark. Three quarters of CISOs say less than a quarter of the pitches they receive are "very good".



Unfortunately, startups seem to be falling at the first hurdle since it is not just a matter of poor presentation or pitching style; the most common mistakes are the fundamentals of selling a product. More than 20% of CISOs frequently see pitches with unclear messaging and 21% report the common mistake of failing to specify what differentiates the product from others.

Few CISOs have noticed gaps around business plans in pitches, and less than 5% reject products because the business seems too risky. It is obvious that startups are good at selling their business ambitions, which has become a key element of any pitch deck. But a lot of improvement is needed on communicating about the product and the use cases.

The most common reason a CISO rejects a product (24%) is because it **doesn't actually solve the problem they were expecting it to**.

When asked open-ended questions about the common mistakes they see in startup pitches, CISOs freely offered comments about confusing or unhelpful information.

Out of the mouths of CISOs

OTHER COMMON MISTAKES CISOS MENTIONED

"Not enough clarity on the market problem, the urgency of the problem, and how pervasive the problem could become"

"Too much focus on the tech, rather than the business solutions"

"Doesn't tell me or show me what the product actually does"

"Unclear value"

"Assuming knowledge, or lack of knowledge, in the audience"

"Lack of real-world application and quantification of efficacy"

Essentially, startups need to do more work to understand CISO priorities, business challenges and product requirements so that they can pre-emptively answer the questions CISOs have before they even have to ask.

KEY TAKEAWAYS FOR STARTUPS

DON'T

- **Withhold important details in the pitch**
- **Overly focus on your ground-breaking technology and neglect the business use-cases**

DO

- **Make sure your messaging is clear, consistent, and easy for a CISO to consume quickly**
- **Specify the business problem you are tackling and how your product stands out from competitors**
- **Be prepared to demo or explain how the product works and provide statistics on its efficacy**
- **Learn about the company you are pitching to and tailor the communication appropriately**

HOW TO SOLVE REAL BUSINESS PROBLEMS

Telling a technology startup to stop focusing so much on technology seems like counterproductive advice, but this is exactly what CISOs unanimously say would improve communication between themselves and technology vendors.

Time and time again, across a number of different survey questions, CISOs petitioned startups to "focus on the business problems" rather than selling their technology.

Out of the mouths of CISOs

ONE TIP FOR CYBERSECURITY STARTUPS (a selection of responses)

- *Think about my business case*
- *Understand industry-specific issues*
- *Come up with a valuable and original idea and commercialise it. Don't worry about the technology initially*
- *Concentrate on what the customer needs and not the product*
- *Clearly articulate which business problem you solve and why you do it better than anyone else*
- *Focus on the problem, not the tech or the solution*

In interviews, the decision-makers explained what they meant in more detail. The key, they said, is to answer the question "how does my product help the cybersecurity team?" and not "what does my product do?". A startup might think it is obvious why it is helpful for a CISO if a product "stops advanced threats", but simply stating a product feature (or result) does not explicitly explain the business value.

> ***"Answer the question "How does my product help the cybersecurity team?" and not "What does my product do?"***

For Paul McKay, it is important that startups address the pressure on CISO's resources when they make their business case, since this is one of the main motivators and priorities across many sectors.

"I always ask vendors to demonstrate the business value, but in response I get a list of technical specifications," he says. "I do also want to know those, but their response often doesn't answer the core challenge CISOs are facing."

Many CISO roles are closer to business strategy than they are to IT and security, explains Alan Jenkins. Ideally - if not for the pressure on resources - CISOs would be looking much further ahead and planning how to build resilience and efficiency and reduce risks in the future.

Vendors need to show CISOs how their products enable the security teams to get on with the strategic part of their jobs.

"As a CISO, if you're always in the response phase, you're behind the problem," he says.

Out of the mouths of CISOs

SOME OF THE BUSINESS PROBLEMS CISOS ARE TASKED WITH

- *How do I do more with less?*
- *How do I achieve greater security with fewer human resources?*
- *How do I stay compliant efficiently?*
- *How do I get oversight of my risks and understand the business impact?*
- *How can I operate quicker or get more sales in without compromising on security?*

CONCLUDING REMARKS

For a new cybersecurity vendor or startup, getting the attention of CISOs who are overwhelmed with pitches might seem like the crux of the challenge, but the tips to stand out from the crowd are easy to implement: no sales calls, appropriate networking and succinct methods of communicating the important product features.

The harder hill for vendors to climb is how to approach cybersecurity the way that CISOs do: as a business problem, with opportunities for greater efficiency, cost-savings, and valuable business insights. To truly create a synergy between a company's cybersecurity team and technology vendors, conversations need to shift from focusing on technology innovation to a deeper engagement with how these technologies will support and improve the business strategy moving forward.

PART 3

TOP TIPS FROM CISOS TO STARTUPS

PART 3

TOP TIPS FROM CISOS TO STARTUPS

PROVIDE IMPORTANT INFO ON YOUR WEBSITE

"Vendors' websites should ideally describe in some detail what their solution does and how it works, but often they don't.
You shouldn't need to ask for contact details just to provide that information. If the site does not provide sufficient detail I am likely to move on, and if my details are required to learn more it is likely I won't follow up."

FIND GAPS IN THE MARKETPLACE

"Spend time understanding where current problems / issues are unlikely to be met by established vendors."

UNDERSTAND THE CLIENT & TAILOR YOUR WORK

"Tailor your proposal to the customer you are speaking to. Listen to what they want and design a solution to that. Be clear about why your product solves their specific problems and challenges in a way that nobody else can in the established marketplace. CISOs will need to expend political capital to convince other colleagues about why they should take the risk of working with a start-up. You need to make it clear why they need to work with you and nobody else."

PART 3

TOP TIPS FROM CISOS TO STARTUPS

FOCUS ON THE BUSINESS, NOT YOUR PRODUCT

- Try to understand the CISO's predicament before you try to sell to them; especially try to understand the breadth and complexity of their role and the great diversity of solutions that they need
- Think about the business case
- Concentrate on what the customer needs and not the product
- Clearly articulate which business problem you solve and why you do it better than anyone else
- Don't get into too much technical detail
- Pitch like you're selling to a business leader and not a techy
- Help the CISO by credibly linking your product to drivers of business value

KEEP IT SIMPLE

- Do one thing well, and describe it clearly
- Come up with a valuable and original idea and commercialise it. Don't worry about the technology initially

PITCHING / SALES TIPS

- Avoid using fear as a tactic
- Ensure that staff selling your product are knowledgeable about cybersecurity and know the product/solution well
- Stop talking about your journey and show me what the product is
- Be honest about what the product does and why it is better than others
- Clarify that you understand the market problem and can solve it in a unique way

• CYLON INSIGHTS •

CYLON

We find, grow and invest in the world's best emerging cyber businesses

For more information about our programmes in London and Singapore, please visit cylonlab.com or contact mail@cylonlab.com

.